FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY
DEPPARTMENT OF CYBER SECURITY SCIENCE
CYBER WARFARE PRACTICE QUESTIONS

Questions by: **Prof. Waziri**
Attempted Solutions by: **M.Tech CyberSecurityScience Students, 2021 set**
Lead Contributor: **Ateata Gabriel**
Documented by: **Hafiz Omeiza Haruna**
Date: 12/11/2022

Cyberwarfare
Additional Practice Questions

1. (a). As a student in the field of Cyber security, what do you concept with the clause "Cyber Warfare"?
   (b). Numerate and discuss succinctly, 5 major types of cyber warfare attacks.
   (c). Give 5 instances of cyber warfare operations you know

2. (a). How can we defend our country against cyber warfare. Please feel free to explain each with practical theoretical examples
   (b). Discuss freely, the future of cyber warfare and cyber security.

Answers

1. (a). **Cyber warfare** is the use of cyber-attack against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems. Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.
   It is used in a broad context to denote interstate use of technological force within computer networks in which information is stored, shared or communicated online.
   It is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state security (actual or perceived).

(b). **Types of cyber warfare attacks**

i) **Malware Attack**: This is one of the most common types of cyber-attacks. "Malware" refers to malicious software virus including worms, spyware, ransomware, adware and Trojans. Malware breaches a network through vulnerability when the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

ii) **Phishing Attack**: Phishing attacks are one of the most prominent widespread types of cyber-attacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails. Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By so doing, attackers gain access to confidential information and account credentials.

iii) **Password Attack**: Password attack is a form of attack when a hacker cracks a user's password with various programs and password cracking tools like Aircrack, Cain Abel, John the Ripper, Hashcat etc. There are different types of password attacks; like Brute force Attack, Dictionary Attacks, and Keylogger Attacks.

iv) **Man-in-the-Middle Attacks (MITM)**: MITM is also known as an Eavesdropping attack. In this attack, an attacker comes in between a two party communication, i.e. the attacker hijacks the session between a client and host. By so doing, hackers steal and manipulate data.

v) **Denial-of-Service Attack (DOS)**: A DOS attack is a significant threat to companies. Here,, attackers target systems, servers or networks and flood them with traffic to exhaust their resources and bandwidth. When this happens, catering to incoming request becomes overwhelming for he servers, resulting in the website hosts to either shutdown or slowdown.

vi) **SQL Injection Attacks**: A structured query Language (SQL) injection attack occurs on a database driven website when the hacker manipulates a standard SQL query. It is carried out by injecting a malicious code into a vulnerable website search box, thereby making the server to reveal crucial information.

c) **Instances of cyber Warfare operations**:

i) **Kaseya Ransom Attack**: Kaseya, a US based provider of remote management software services, experienced a supply chain attack, which was made public on July 2, 2021. The company announced that attackers could use its VISA product to infect customers' machines with ransomware.

ii) **Solarwinds Supply Chain Attack**: This was a massive, highly innovative supply chain attack detected in December 2020 and named after it's victim, Austin-based IT management company, Solarwinds. It was conducted by APT29, an organized cybercrime group connected to the Russian Government. The attack compromised an update meant for Solarwinds software platform, onion. During the attack, threat actors injected marlware, which came to be known as **Sunburst** or **Solorigate Malware** into onion's updates. The updates were then distributed to Solarwinds customers.

iii) **Amazon DDOS attack**: In February 2020, Amazon web services (AWS) was the target of a large scale Distributed-Denial-of-Service (DDOS) attack. The company experiences and mitigated a 2.3Tbps (Terabits per second) DDOS attack, which had a packet forwarding rate of 293.1Mpps (Million packets per second).

iv) **Microsoft Exchange Remote Code Execution Attack**: In March 2021, a large-scale cyberattack was carried out against Microsoft Exchange, a popular enterprise email server. It leveraged four (4) separate zero-day vulnerabilities discovered in Microsoft Exchange Servers. These vulnerabilities enable attackers to forge untrusted URLs, use them to access an Exchange server system, and provide a direct server-side storage path for malware.

v) **Twitter Celebrities Attack**: In July 2020, Twitter was breached by a group of three attackers, who took over popular Twitter accounts. They used social engineering attacks to steal employee credentials and gain access to the company's internal management systems, later identified by Twitter as **Vishing** (Phone Phishing).

2) (a). **How to defend the nation against cyber warfare**

i) **Avoid acquiring technology from companies based in Nations that pose a threat**. Such avoidance should not be interpreted to that buying from domestic entities that don't have sufficient-supply-chain security control in place is acceptable. We need to be aware of how things (technologies) are made, not just where they are made.

ii) **Isolationism**: Perhaps the safest way to protect data is to remove internal systems from the internet entirely. Access to the internet should optimally be physically isolated from the internal network with one-way tightly secured paths to more data into and out of the internal network.

iii) **Share cyber threat information**: Sharing of cyber threat information among businesses, as well as between Government and business could help mitigate attacks from nation-states. What they are trying to do is get companies to upgrade their information security systems substantially, and those that can or will make the necessary upgrade are rewarded by gaining access to truly high-level data.

iv) **Enhance Security Awareness**: There should be regular training of personnel and testing employees about proper cyber hygiene awareness.

b) The future of cyber Warfare and Cyber Security;

Over the years, we have seen an escalation in the series of hacks on healthcare services, power grids, nuclear plants and our privacy, with no respite. This intent is to destabilize a country. We live in a highly connected world. These connections are themselves connected to grids that manage the network efficiently. Be it the energy grid, the finance grid or transportation grid, all are connected, interdependent and sometimes, connected to a super grid. However, a super connected smart nation also means security threats that have potential to destabilize, or at least disrupt the country. A potential vulnerability on one grid can have a multiplier effect that impacts them all.

Cyber Attacks will be the new battlefield – unseen, invisible and unpredictable, where hackers from various nations will compete to disrupt economies and lives.

The future seems grim, as recent reports reveal state-sponsored cyber warfare tactics is increasingly difficult to trace an incident back to a specific country. Thus, countries are now collaborating and innovating to counter such attacks. The future may see a full-blown cyberwar if the uncertainty around global cyber-security regulations persist.